CLAIMS

We claim:

1. A method for ensuring integrity of data, comprising:

separating an amount of data into segments;

computing a cryptographic checksum for a said segment; and

combining a segment and an associated cryptographic checksum into a data packet.

2. The method described in Claim 1 wherein said data comprises media data.

3. The method described in Claim 1 wherein said data comprises secure scalably streamable data.

4. The method described in Claim 1 wherein said data is transmittable in a network.

5. The method described in Claim 1 wherein said data is stored in a storage medium.

6. The method described in Claim 1 further comprising applying a header to said data packet.

7. The method described in Claim 1 further comprising forwarding said data packet.

8. The method described in Claim 1 wherein said media data to be streamed comprises a plurality of said data packets.

9. The method described in Claim 1 further comprising encrypting said segment and said cryptographic checksum.

10. The method described in Claim 9 wherein said packet is enabled to be decrypted independently of other packets comprising said streamed media data.

11. The method described in Claim 1 wherein said cryptographic checksum is computed for a truncatable unit in said segment.

12. The method described in Claim 11 wherein said segment comprises a plurality of said truncatable units.

13. The method described in Claim 12 wherein a cryptographic checksum is computed for each of said truncatable units in said segment.

14. The method described in Claim 12 wherein a first cryptographic checksum is calculated for a first truncatable unit, and wherein a second cryptographic checksum is calculated for the combination of a second truncatable unit, said first truncatable unit, and said first cryptographic checksum.

15. The method described in Claim 1 wherein said cryptographic checksum is computed using a hash function.

16. A method for providing security to a scalably streamed media signal in a network, comprising:

separating said streaming media signal into a plurality of truncatable units;

computing a cryptographic checksum for each of said truncatable units;

appending said associated cryptographic checksum onto each of said truncatable units;

combining one or more of said truncatable units and associated cryptographic checksums into a transmittable data packet; and

forwarding said data packet.

17. The method described in Claim 16 further comprising applying a transcoder-readable header to said data packet.

18. The method described in Claim 17 wherein said transcoder-readable header is enabled to be read without decrypting encrypted parts of said data packet.

19. The method described in Claim 16 wherein a cryptographic checksum is computed for each truncatable unit in said segment.

20. The method described in Claim 16 wherein a first cryptographic checksum is calculated for a first truncatable unit, and wherein a second cryptographic checksum is calculated for the combination of a second truncatable unit, said first truncatable unit, and said first cryptographic checksum.

21. The method described in Claim 16 wherein the size of said truncatable units is selected to ensure the size of said data packet is transmittable in said network.

22. The method described in Claim 16 wherein said associated cryptographic checksum is computed independently for its associated truncatable unit.

23. The method described in Claim 16 further comprising encrypting each of said truncatable units.

24. The method described in Claim 16 wherein said cryptographic checksum is calculated using a hash function.

25. The method described in Claim 16 further comprising:

accessing said data packet;

reading a transcoder-readable header of said data packet;

deleting one or more of said truncatable units; and

forwarding said data packet.

26. The method described in Claim 25 further comprising:

writing a new transcoder-readable header for said data packet reflecting said deleting; and

applying said new transcoder-readable header to said data packet.

27. The method described in Claim 25 wherein said transcoder-readable header is enabled to be read without decrypting encrypted parts of said data packet.

28. The method described in Claim 25 wherein said deleting comprises transcoding said data packet.

29. The method described in Claim 25 wherein said transcoder-readable header comprises information related to the content of said data packet while leaving said truncatable units undecrypted.

30. A computer readable medium having a data packet stored therein for causing a functional change in the operation of a device, said data packet comprising:

a plurality of truncatable units, each of said units comprising an amount of media data; and

a cryptographic checksum computed for each of said truncatable units.

31. The computer readable medium described in Claim 30, wherein said data packet further comprises a transcoder readable header comprising information related to said truncatable units and said cryptographic checksums.

32. The computer readable medium described in Claim 31, wherein said transcoder readable header enables transcoding said data packet.

33. The computer readable medium described in Claim 31, wherein said truncatable units and said cryptographic checksums are enabled to be encrypted independently of said transcoder readable header.

34. The computer readable medium described in Claim 31, wherein said truncatable units and said cryptographic checksums are enabled to be decrypted independently of said transcoder readable header.

35. The computer readable medium described in Claim 31, wherein said transcoder readable header is enabled to be read independently of said truncatable units and said cryptographic checksums.

36. The computer readable medium described in Claim 30, wherein said cryptographic checksum is computed based on one truncatable unit.

37. The computer readable medium described in Claim 30, wherein said cryptographic checksum is computed based on a plurality of truncatable units and associated checksums.

38. The computer readable medium described in Claim 30, wherein said cryptographic checksum is calculated using a hash function.

39. The computer readable medium described in Claim 30, wherein said cryptographic checksum is calculated using a message digest function.

40. The computer readable medium described in Claim 30, wherein said cryptographic checksum is calculated using a message authentication code function.

41. The computer readable medium described in Claim 30, wherein said cryptographic checksum is calculated using a keyed-hashing-for-message-authentication function.

42. The computer readable medium described in Claim 30, wherein said cryptographic checksum is calculated using a digital signature function.

43. The computer readable medium described in Claim 30, wherein said transcoder readable header is enabled to be written

independently of said truncatable units and said cryptographic checksums.

44. The computer readable medium described in Claim 30, wherein each of said truncatable units is enabled to be deleted from said transmittable packet independently of other truncatable units in said packet.